

2 4 12 14


# chp5 <sup>8</sup> <sup>15</sup> after Test Software Fault Tolerance

الأسباب الأساسية لوجود أخطاء في البرمجيات

- # why software are <sup>defect</sup> prone ??? <sup>أخطاء برمجية</sup>
- # why problem of designing sw very difficult ??? <sup>تصميم</sup>

There are difficult problem

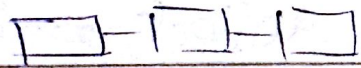
- 1/ <sup>أساسي - ضروري</sup> Essential
- 2/ <sup>عرضي</sup> Accidental

 Essential diff <sup>arise</sup> come from: <sup>أسباب</sup>

- 1/ <sup>understanding</sup> a complex system <sup>app</sup> → need some experience to translate to design a sw




2/ The system construct have

multi stage with 

default transition rules

3/ SW must be modify according to the How

 Accidental & —

People making mistake even the system is simple.

تحويل التفاصيل الدقيقة  
code

— Transliteration of the details design

من تصميم إلى كود

• design mistake

بعد اقله الجزء المسمى كذا

قبل Fault redundancy (Acceptance test)

هناك نقطة فيها وكذا نقطة

من ان تحقق هدف معين لا نشق اخطاء

SW

\* A Cceptance test & — is essentially a check of reasonableness

1/ Time checks: how long this program is running for how long time.



## 2/ Verification of output

مثلاً - هنا الناتج لم يتطابق معرفة وجود defect

$$\sqrt{146} = 12.xx$$

التعليق له انه

من الخارج نتبع المداخله الى اساسه (المعنى) وتقارن هذا بغيره الى اصل امر لا

## 3/ Range checks

ايضا القيمة السالبة القيمة  
مقبولة

42

43

55

45

~~Single~~ Vartron Fault Tolerance

نحاول تقوية الى مستوى الواحدة اقوى

منه الى تقوية المشاغل وذلك عن

robust

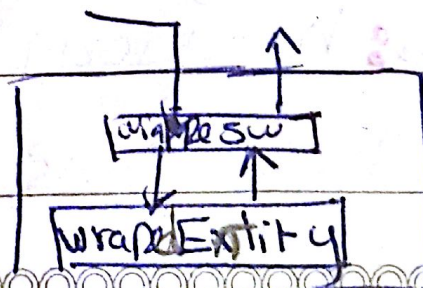
طريق

## 1/ Wrapper

encapsulation for the sw

by another sw to make it

strong





# Commercial off-the-shelf (COTS)

Software <sup>for</sup> component high reliability

For general purpose

① - dealing with buffer استقبال - wrapper

② - checking the correctness of the schedule

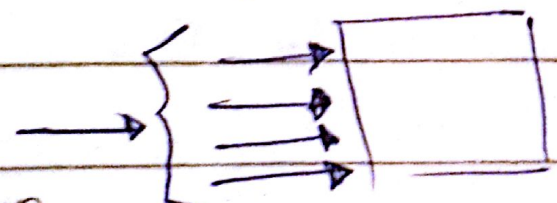
hang تحقق من صحة الجدول

يتميز الشيء الذي لم يكن فيها لأخطاء حتى لا يندفع

③ - using SAT

using sw with known bugs

④ - using wrapper to check correct o/p



⑤ - Quality of Acceptance Test (AT)

⑥ - reliability of information

⑦ - Extent to which the wrapped sw module has been tested  
~~Extent~~ the ~~weight~~

\* differentiate between Essential

Accidental

\* Define wrapper and write three area of its application

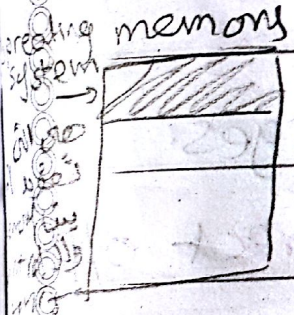


# Software Rejuvenation

العمليات التي تقوم بعملها على حساب  
hanging للموسم (تفعلها) restart  
(rebooting)

ما هو الشيء الذي تقوم به hanging

الموسم A, B, C, D, E, F, G, H



RAM

A	B
E	D

in execution  
شأنه في التنفيذ

Save Error RAM

إذا كانت في حالة خطأ فتم حفظها في RAM

error في بعض العمليات

correct for error

rebooting down

Process

terminate any Process that is in  
excution



# Rejuvenation level

Application

Process

سؤال \* Suspending of the specific app.   
 effect all app - rebooting the process

cleaning up its state

\* reinitialization of data structures.

Rejuvenation based in two types   
 (time or prediction)

Time-based rejuvenation e-

cost of each error

cost of each rejuvenation

$$C_{rejuv}(P) = \tilde{N}(P) C_e + C_r$$

inter-rejuvenation Period

$$C_{rate}(P) = \frac{C_{rejuv}(P)}{p}$$

cost per unit time =  $\frac{\text{expected Num of error}}{p} C_e + C_r$



we are running after using sw  
by using hw redundancy.

تنبؤ Prediction

\* monitoring to what happen  
to the (sw)

\* monitoring to system

characteristic الخصائص للنظام

vercal memory في الذاكرة : تتفقد وسيلة  
is low more memory E, F

A	B
C	D

need input.  
need interup

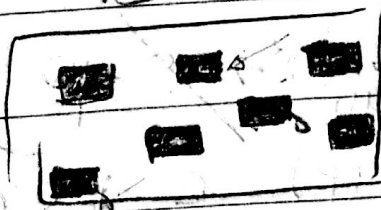
نحتاج بدل E و F ونحقق ان شئ ووفقا

في تنبؤه (توقعنا اننا انشأنا ثغرة)

monitoring space واحد (up normal, error)

Data Diversity تنوع

small  
scattered  
Failure  
region



large contiguous Failure  
region

diversity يوجد تنوع Fault tolerance  
النسبة المئوية



according to size of fault we can decide what Fault tolerance to use.

The input of Process is Fail

الخطأ  
والتي  
منها



المساحة area not enough

{ has error in the hardware

\* region of Failure or non Failure

→ diversity

IF we use acceptance test and

we find error we can

reloading the result or reevaluate

the result

الاستقبال الكافي من أجل اختبار acceptance test

النتيجة



Soft ware Implemented

Hardware Fault tolerance

(SIHFET) to detect HW, ~~HW~~ Fault

Data diversity can be combined with time redundancy

Data diversity & acceptance & detection

Time redundancy use for

Fault correction

(الوقت مع كل ما في نظام)

Information redundancy need Hardware redundancy (need extra)

is expensive and this solved by software



Sys is design to do specific serving

## Dependable system :-

إذا أدى النظام الوظيفة التي صمم لها لمحت  
ات تتعلق على النظام dependable

If system doing the tasks that is designed for it

\* dependability can be :-

✓ **Availability** :- ready ness of correct serv

✓ **Reliability** :- continuas of correct serv

✓ **Safety** :- The absent of a dangers  
on the user or enviroment

عدم وجود شيء  
يؤثر على المشقة  
وعلى البيئة

✓ **Confidentiality** :- مع استناد الخصوصية  
عدم التأثر في النظام  
un override Person (person who is not private)

✓ **Integrity** :- The absent of modification  
or change on the system

(impropre change) of the sys تغير غير ايجابي

✓ **maintability** :- ability the system

that is can modify and repair.

ability to check the default and repair

or replace or modify or reconfiguration  
reactivation

availability + Integrity + confidentiality → security



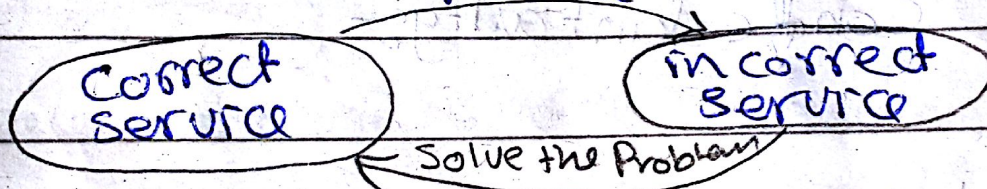
system & collection of component  
such as sw & Hw (op<sup>sw</sup> realting  
sys app --) user

**\* Threat to dependability \***

( Failure, error, Fault )

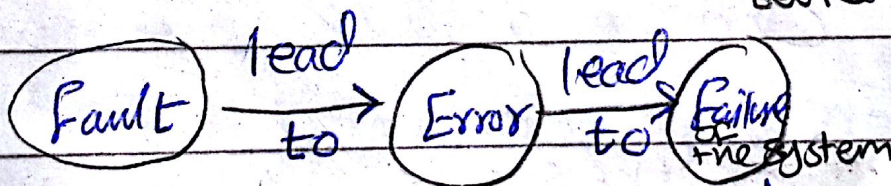
Fault → It can be internally

Failure



Restoration

Transition of incorrect  
service to correct  
service



The main goal is  
how to achieve a dependability  
of system.



وسائل  
للحصول على  
النتائج

## \* Means of achieving dependability

we try to avoid fault, errors, Failure

### 1/ Fault prevention techniques :-

we try to avoid Fault

تجنب حدوث الأخطاء في

Component design review

Quality control

### 2/ Fault tolerance techniques :-

ability of the system to do

or executed task perfectly correctly regardless

the HW ~~defect~~ errors or SW mistakes

we use

redundancy

HW, software, Time, Info

### 3/ Fault removable techniques :-

we try to remove all fault

prediction  
of fault

Forecasting

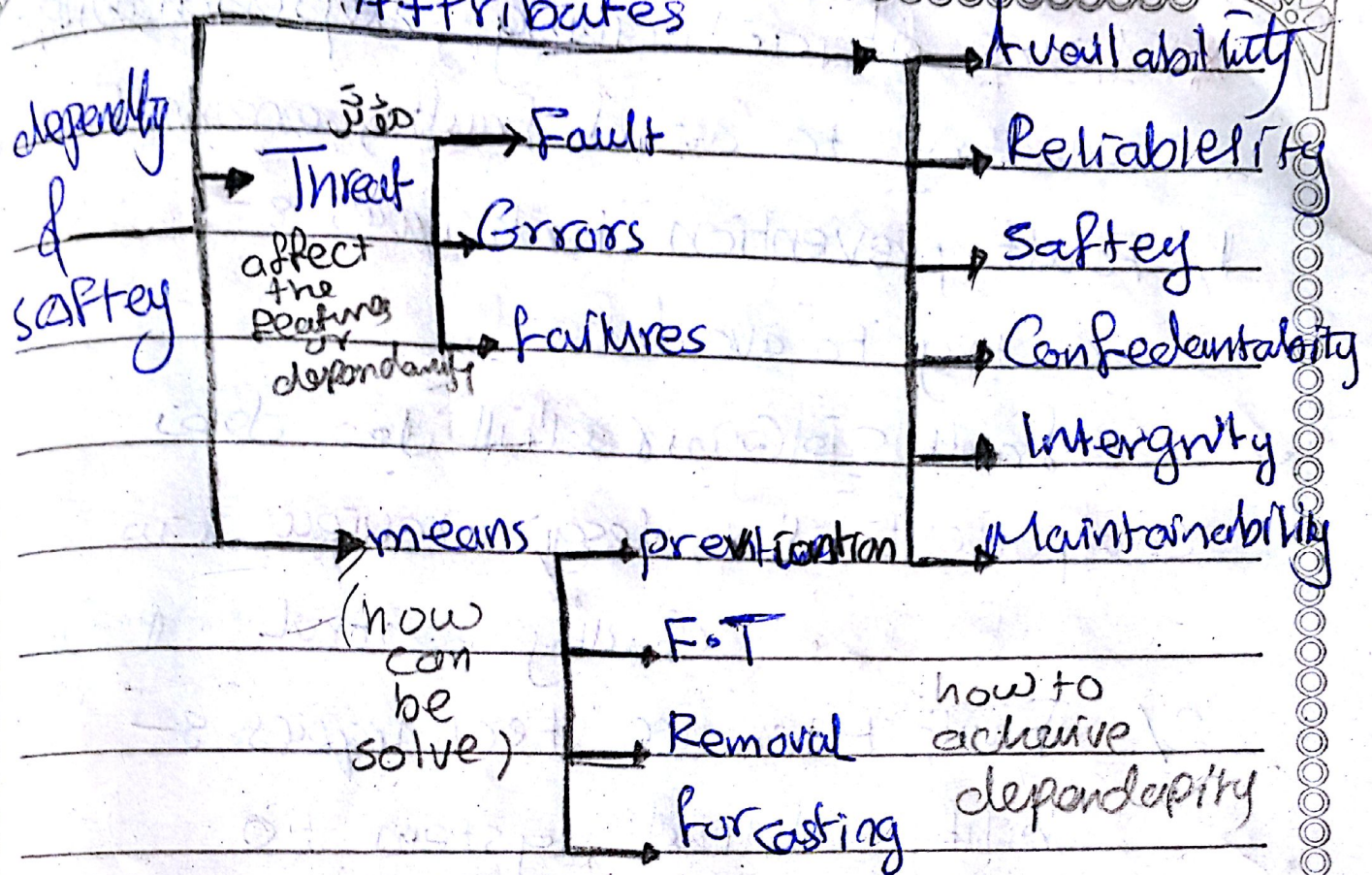
we try to avoid by predicting the fault that is can be

## \* Dependability tree :-

استراتيجية  
على مستوى  
الوقت  
Fault  
tolerance



## Characteristic Features Attributes



Fault prevention techniques is tended to

keep the fault out of system. (by using high reliable component)

high reliable system & sw.

تقنيات منع الأخطاء Fault prevention techniques

## Organization of fault

### Tolerance

The phase of F-T

— error detection

— damage After error



## Damage assessment (evaluation of damages)

- diagnoses & <sup>component</sup> Postmortem <sup>تشخيص</sup>

- reconfigurations

- error recovery (restart)

by time redundancy like transient error.

- Fault Removal & Fault diagnoses  
to remove the fault you must know which part  
Faulty component <sup>is faulty</sup> <sup>لقد نصحنا</sup> <sup>الجذر</sup>

Important Features <sup>صفات</sup>  
to achieve dependability

Coordination & - how to coordinate  
between different component

Signaling & by exception (Prediction)  
of it component

Fault forecasting & <sup>تنبؤ</sup> <sup>علا</sup> <sup>استدلال</sup>

في المستقبل ووصف في البيان

micro  
processor  
RAM